UNIVERSITÀ DI PARMA
Dipartimento di Ingegneria e Architettura

# Vulnerabilities and attacks

Luca Veltri

(mail.to: luca.veltri@unipr.it)

Course of Cybersecurity, 2022/2023

http://www.tlc.unipr.it/veltri

# Vulnerabilities

- Vulnerability (Def.):
  - **[NIST Glossary]: "Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source"**
  - **[IETF RFC4949]: "A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy"**
- The exploitation of a system vulnerability may let an attacker to carry out unauthorized actions against the Confidentiality, the Integrity or the Availability of the system related assets

# Vulnerabilities (cont.)

- Most systems have vulnerabilities, however not every vulnerability results in an attack, and not every attack succeeds
  - **success depends on the degree of vulnerability, the strength of attacks, and the effectiveness of any countermeasures in use**
  - **if the attacks needed to exploit a vulnerability are very difficult to carry out, then the vulnerability may be tolerable**
- Useful archives:
  - **Common Weakness Enumeration (CWE)**
    - https://cwe.mitre.org
    - list of common software and hardware security weakness types
  - **Common Vulnerabilities and Exposures (CVE)**
    - https://cve.org
      - search: https://cve.mitre.org/cve/search_cve_list.html
    - list of publicly known cybersecurity vulnerabilities
    - each entry contains an identification number and a description

# Vulnerabilities (cont.)

- Vulnerabilities can be distinguished based on:
  - **nature**
    - unintentional (e.g. bugs and flaws)
    - intentional (e.g. backdoors)
  - **domain**
    - technology
      - design or specification
      - software/hardware implementation
    - operation and management
      - Inadequacy of organizational aspects in terms of: defense infrastructures, attacks detections, incident response
      - Ineffective security strategy in terms of: best practices, tools, technologies
    - human
      - bad behaviors
      - social engineering
        - psychological manipulation of people into performing actions or divulging confidential information

# Technology vulnerabilities

- Network and communication protocol vulnerabilities
  - **protocol specification flaws**
  - **protocol implementation flaws**
  - **misuses**
    - e.g. unsecure communication protocols, exploitation of address resolution mechanisms (e.g. ARP or DNS), dynamic configuration protocols (BOOTP/DHCP), etc.
- Software and hardware vulnerabilities
  - **Application implementation flaws**
  - **Operating system flaws**
    - OSs are the main sources of reported system vulnerabilities
  - **Hardware flaws**

# From vulnerabilities to attacks

- If a vulnerability in a system is known or discovered and reachable, it can lead to an attack
  - **exploitation of the vulnerability**
- The success of an attack can further lead to another attack
- Examples of vulnerabilities that lead to different types of attacks:
  - **Open ports on outward facing Web and other servers, and code listening on those ports**
  - **Services available on the inside of a firewall**
  - **Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats**
  - **Interfaces, SQL, and Web forms**
  - **An employee with access to sensitive information vulnerable to a social engineering attack**

# Attack Surfaces

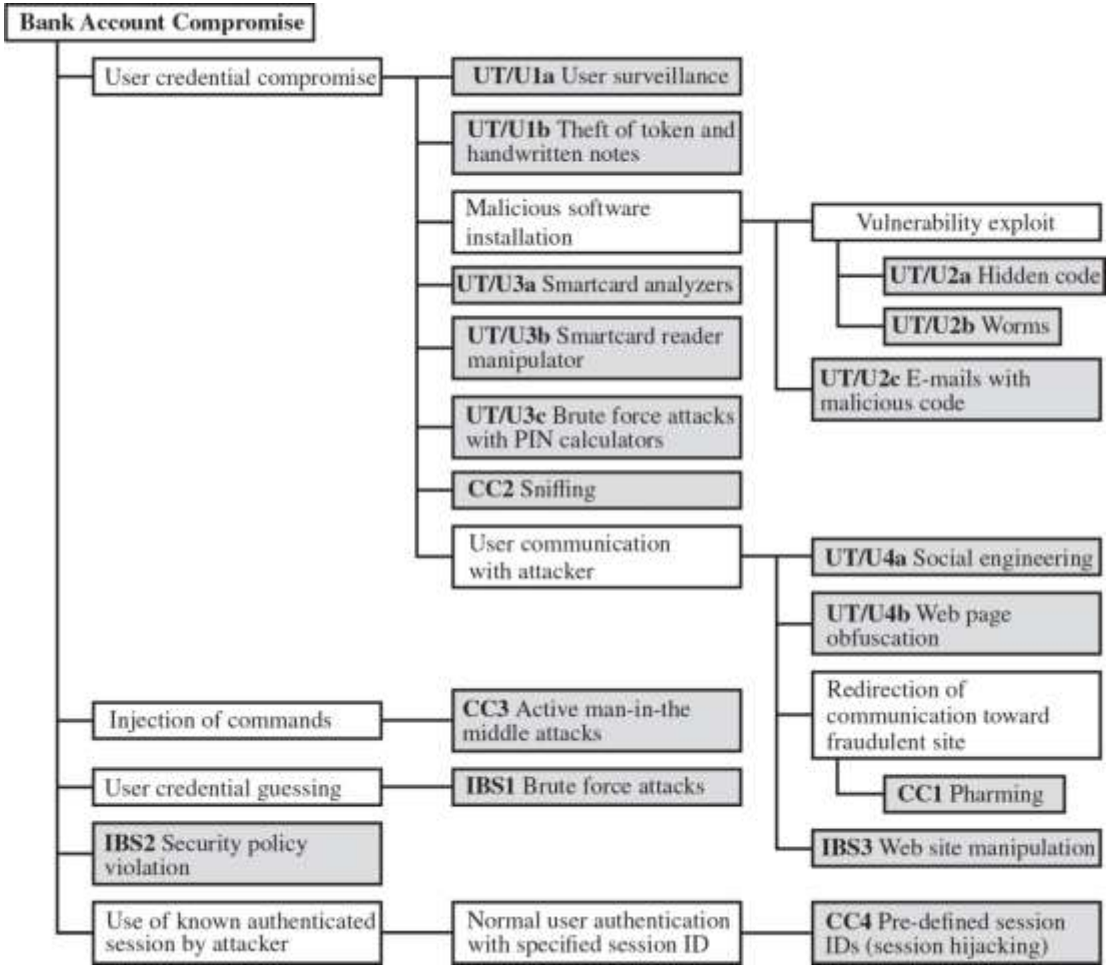
- Network Attack Surface
  - **Vulnerabilities over an enterprise network, wide-area network, or the Internet**
  - **Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks**
- Software Attack Surface
  - **Vulnerabilities in application, utility, or operating system code**
  - **Particular focus is Web server software**
- Human Attack Surface
  - **Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders**

# Attack Tree

- A branching hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities
  - **the security incident that is the goal of the attack is represented as the root node of the tree**
  - **the ways that an attacker could reach that goal are iteratively and incrementally represented as branches and subnodes of the tree**
- Each subnode defines a subgoal, and each subgoal may have its own set of further subgoals, etc
- The final nodes on the paths outward from the root, represent different ways to initiate an attack
- Each node other than a leaf is either an AND-node or an OR-node
  - **branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared**

# Example of an Attack Tree

- Example of an Attack Tree for internet banking authentication:



- Bank Account Compromise
  - User credential compromise
    - UT/U1a User surveillance
    - UT/U1b Theft of token and handwritten notes
    - Malicious software installation
      - Vulnerability exploit
        - UT/U2a Hidden code
        - UT/U2b Worms
      - UT/U2c E-mails with malicious code
    - UT/U3a Smartcard analyzers
    - UT/U3b Smartcard reader manipulator
    - UT/U3c Brute force attacks with PIN calculators
    - CC2 Sniffing
    - User communication with attacker
      - UT/U4a Social engineering
      - UT/U4b Web page obfuscation
      - Redirection of communication toward fraudulent site
        - CC1 Pharming
      - IBS3 Web site manipulation
  - Injection of commands
    - CC3 Active man-in-the middle attacks
  - User credential guessing
    - IBS1 Brute force attacks
  - IBS2 Security policy violation
  - Use of known authenticated session by attacker
    - Normal user authentication with specified session ID
      - CC4 Pre-defined session IDs (session hijacking)

- UT/U: attack targets the user terminal, including smartcards, and actions of the user
- CC: attack focuses on communications channel
- IBS: attacks against the Internet banking servers

# Computer Security Strategy

- A comprehensive security strategy involves three aspects:
  - **Security Policy**
    - formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources
  - **Security Implementation**
    - involves four complementary courses of action:
      - Prevention
      - Detection
      - Response
      - Recovery
  - **Assurance and evaluation**
    - encompasses both system design and system implementation
    - assurance is an attribute of an information system that provides grounds for having confidence that the system operates such that the system's security policy is enforced
    - evaluation is the process of examining a computer product or system with respect to certain criteria
      - involves testing and may also involve formal analytic or mathematical techniques